White Paper

ArrayOS: A Hardened, Secure Operating System

Array Networks Network Functions Platform, ADC,
Web Application Firewall & SSL VPN Solutions

Introduction

Network and data center attacks are ever-evolving and gaining in complexity and sophistication quickly over time. Security has become a critical issue for IT managers, and even more so for those who must meet the requirements of regulations such as PCI-DSS, HIPAA and others. Any network or security appliance that is exposed to the internet is a potential subject of cybersecurity attacks such as protocol or flood attacks, break-in attempts and other malicious actions. Without hardening, these network and security appliances will not survive these attacks – and the servers, resources and services behind these appliances will thus also be compromised.

From the company's beginnings, Array has maintained a rigorous focus on security; for example, Array developed a proprietary SSL stack that is used for all production traffic across all Array product lines. The Array SSL stack has proved immune to the vast majority of SSL vulnerabilities such as Heartbleed, Bash, POODLE and others, unlike other solutions that rely upon the open-source OpenSSL for their respective SSL stacks.

Array's stringent focus on security extends throughout every Array network functions platform, application delivery controller, SSL VPN and other products, as well. Because Array's products are typically deployed as a front-end to critical business applications or resources, and are connected to public IP addresses directly accessible from the internet, they too can be a target for cybersecurity attacks.

The core operating system running on Array Networks' appliances – ArrayOS – therefore needs to offer not only optimized application delivery, secure remote and mobile access and other services, it also needs to operate in a highly secure manner in a non-stop operation environment.

Security at the Core

The ArrayOS is a purpose-built and customized operating system that is configured as a secure embedded/real-time network OS. This customization includes a number of key security strategies. ArrayOS will only respond to configured services – the OS is wiped clean of any unnecessary functions, network services and applications. The use of 3rd-party libraries and tools is kept to a minimum – the ones in use are thoroughly screened, validated for their security postures and kept up to date in order to maintain their secure postures. Access to the platform is shut off for everything except device management for service administration.

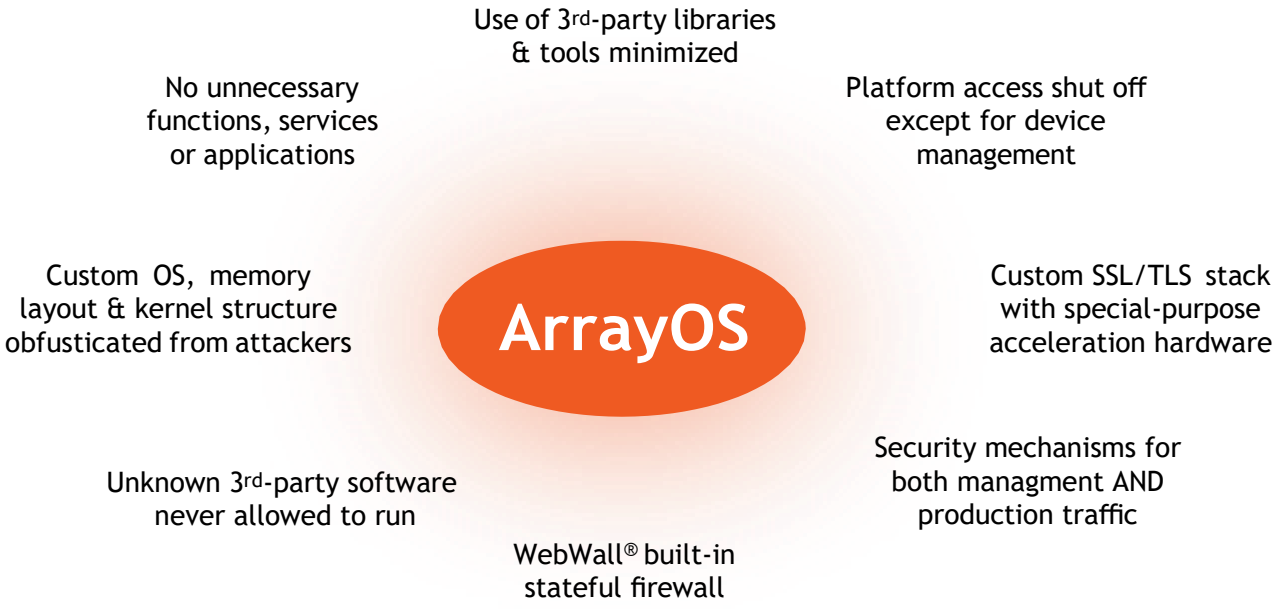

Figure 1: Key ArrayOS security strategies

The customized network operating system also ensures that the memory layout and kernel structure cannot be anticipated by attackers for use as threat vectors. In addition, ArrayOS has a built-from-ground-up TCP stack that has matured and been tuned over almost 20 years, meaning that ArrayOS is not vulnerable to common Layer-4 attacks. As mentioned previously, ArrayOS also includes a fully custom-built SSL/TLS stack that uses special-purpose acceleration hardware. The result is that ArrayOS is not vulnerable to the vast majority of SSL/TLS vulnerabilities.

The ArrayOS provides its own custom Cisco IOS-like CLI shell and WebUI for managing its functionality. While both management options provide full control of the accessible functions of the Array appliance, neither permits unknown third-party software to run – in order to prevent malicious attacks via this potential vector. Thus the risk of vulnerabilities caused by loading malicious software is reduced to the least possible exposure. For example, while Array's dedicated appliances exclusively use Intel processors, they are not affected by the Meltdown and Spectre vulnerabilities.[1]

[1]Array's vAPV virtual ADC, vASF virtual WAF/DDOS and vxAG virtual SSL VPN, while not directly affected by these vulnerabilities, may be affected if the hosting environment (i.e. VMware, KVM, etc.) is vulnerable.

A Deeper Dive into ArrayOS Security Hardening

The ArrayOS features hardened security for both management and production traffic to support non-stop operation. In particular, security mechanisms for management traffic include:

- Physical console access is allowed only for administrators to access the ArrayOS CLI. However, administrators (and others) are prevented from accessing the customized BIOS and firmware or from changing the startup settings. In addition, no back doors are present or ever allowed.
- Network management access can be explicitly configured to allow access only by trusted clients. All network management access is encrypted using SSH or HTTPS, including the CLI and WebUI, XML-RPC, SOAP and RESTful API.
- Passwords are stored using non-reversible encryption.
- To prevent potential brute-force password attacks, remote management access to a network-connected device needs to be explicitly granted.
- No two device/system/support access passwords are the same. If field support requires access for remote diagnostics and troubleshooting, for example, the administrator must contact Array for a dynamic password.

The ArrayOS supports a number of features to ensure continuous operation as well:

- Each system includes two bootable partitions, which is a useful feature for field software updates and for recovery if one of the partition's software becomes corrupted.
- Hardware/software watch dog timer (WDT) supports reloading of software to prevent system hangs.
- At-a-glance LED lights on the system's front panel indicate power-up, running mode, and fault mode.
- Built-in redundancy with VRRP (Virtual Router Redundancy Protocol) or high availability supports multiple units.

Like management traffic, production traffic on an Array appliance offers security designed in from the ground up. For example:

- ArrayOS features customized kernel processing logic and uses memory pools. This customization means that it is highly unlikely for attackers to detect the memory layout and kernel structure and use them as threat vectors. For example, the memory pools are partitioned and pre-allocated. In addition, under attacks such as DoS or DDoS, the kernel operation and memory usage is bounded, which provides better system usability and stability.
- To support millions of active/full TCP connections and high performance, ArrayOS utilizes a custom packet processing scheme (Array's SpeedCore®, a custom transmission control protocol

(ATCP)). Array routinely stress tests ATCP, and scans it with network scanning and attack tools to ensure compatibility and immunity from known network attacks, such as L4 TCP SYN flood, TCP Zero Window attacks and many others.

- At the Layer-2 level, ArrayOS includes a built-in stateful firewall called WebWall. WebWall can be configured to filter all ingress packets, thus permitting access only from selected clients. With WebWall, zero-day exploit threats via packets are nonexistent.
- As mentioned previously, Array's custom SSL/TLS stack, integrated with special-purpose SSL acceleration hardware, makes ArrayOS SSL processing of production traffic immune to the vast majority of OpenSSL and other SSL/TLS vulnerabilities.

A Layered Security Approach

In addition to the security afforded by ArrayOS itself, most Array product lines include multiple other security mechanisms relevant to those devices' respective roles. For example, the APV and vAPV application delivery controllers can be deployed in forward- or reverse-proxy mode to protect traffic, and can also operate as a Webagent service to implement explicit forward proxy mode for additional security.

All Array ADCs include DDoS protection for server load balancing, with machine learning to analyze traffic patterns and automatically configure HTTP and DNS thresholds to protect against anomalous traffic. Defense is provided across a wide range of protocol and network attacks. In addition, HTTP and DNS access control lists can be implemented at the administrator's discretion, and an ACL blacklist can also be utilized.

Array's ADCs also offer as an option the Webroot BrightCloud Threat Intelligence Service, which offers reputation services to protect users from malicious websites. BrightCloud also includes an optional web classification service to allow blacklisting of inappropriate or dangerous sites, and whitelisting for sites to which traffic has to flow without inspection – for example, banking, healthcare and other sites that handle personal confidential information.

APV and vAPV ADCs support secure application access via Security Assertion Markup Language (SAML), LDAP, RADIUS and OAuth, allowing users to sign on a single time and gain access to applications to which they authorized to access. Single log-out will close all open logins at the end of a session, ensuring security. APV and vAPV also support a broad range of client/server certificate management, client certificate authentication and authorization, and client certificate application integration tools.

In addition, APV and vAPV offer 'Password forcemode' to bolster access control security. When activated, this mode enforces specific rules for admin accounts. New admin passwords must meet length and character requirements, and existing ones must follow these rules when changed. Additionally, new admin accounts must change their passwords on the first login. If the default admin password isn't updated or a factory reset occurs, it must be changed on the next login. The system adds security by temporarily locking accounts after five failed logins, checking password

history to prevent reuse, and setting a 90-day password expiration. These rules apply only when the password change force mode is enabled, enhancing system security.

Array Networks SSL VPN appliances (the AG Series dedicated appliances and vxAG virtual appliances) offer a wide variety of security mechanisms for client devices, for data in transit, and for the network and its resources. Client-side security includes host checking, adaptive policies, cache cleaning on session termination, and end-point security mechanisms. Server-side security includes content filtering, DDoS protection with deep packet inspection, and reverse-proxy network separation, in addition to support for multiple SSL and ECC encryption protocols.

The AG Series and vxAG SSL VPNs include a full range of authentication, authorization and auditing (AAA) tools, and offer a built-in one-time password mechanism as well as supporting multiple third-party multifactor authentication solutions.

Array's DesktopDirect remote desktop access option allows employees to control their physical and virtual desktops from any remote location with internet access. With this option, sensitive files and data never leave the corporate network and never reside on remote or mobile devices to assure security while allowing remote workers to access needed resources.

Array Networks ASF Series employs the sophisticated 64-bit SpeedCore™ multi-core processing architecture, providing comprehensive detection and defense against attacks and threats for business-critical applications. Combining the negative and positive WAF models together, Array Networks ASF Series can not only detect and block the latest known attacks and security vulnerabilities but also effectively prevent "Zero-day" attacks. vASF virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments, offer infrastructure services and new elastic business models or evaluate Array application security firewall with minimal risk.

Summary

IT managers of enterprise and service-provider networks and data centers face a daunting challenge in keeping their corporate resources safe against ever-evolving threats. Ensuring that internet-facing network elements are based upon an operating system that is security-hardened against potential attacks is an important first step in an overall security strategy.

ArrayOS, the proprietary operating system used in Array application delivery solutions, is designed from the ground up as a hardened, embedded real-time operating system. ArrayOS was conceived and crafted from the perspective of security, and this philosophy has continued throughout Array's history. In addition, ArrayOS security hardening extends outward to management access, to non-stop operation, and to production traffic. These security strategies are complemented by role-specific security mechanisms in Array's application delivery solutions.

Through ArrayOS, IT managers can be assured of optimized application delivery, secure remote and mobile access and other services, as well as highly secure environments that support non-stop operations.

About Array Networks

Array Networks solves performance and complexity challenges for businesses moving toward virtualized networking, security and application delivery. Headquartered in Silicon Valley, Array addresses the growing market demand for Network Functions Virtualization (NFV), cloud computing, and software-centric networking. Proven at more than 5,000 worldwide customer deployments, Array is recognized by leading analysts, enterprises, service providers and partners for pioneering next-generation technology that delivers agility at scale.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

Taiwan
Support-taiwan@arraynetworks.com
886-2-27846000

France and North Africa
infosfrance@arraynetworks.com
+33 6 07 511 868

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@arraynetworks.com
+81-44-589-8315

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866 MY-ARRAY (692-7729) or authorized reseller.